REMARKS/ARGUMENTS

Claims 1-20 are pending. Claims 1 – 20 stand rejected. Reconsideration of this application is requested.

Rejection of Claim 1 under 35 USC 103(a) as being unpatentable over Wasilewski (U.S. Patent 6,424,714) in view of Hendricks (U.S. Patent 5,600,364)

Claim 1 stands rejected under 35 USC 103(a) as being unpatentable over Wasilewski in view of Hendricks. Applicant requests reconsideration and removal of this rejection for at least the following reasons. To establish a prima facie case of obviousness, all of the recited claim limitations must be taught or suggested in the prior art (See MPEP §2143.03). Further, there must be some suggestion or motivation, and reasonable expectation of success, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine reference teachings (See MPEP §706.02(j)).

Applicant submits the combined teachings of Wasilewski and Hendricks, as applied in the Final Office action, fail to teach each of the limitations recited in present Claim 1.

Amended Claim 1 recites:

> A method for managing access to a scrambled event of a service provider, said method comprising:
>
> receiving in a device an electronic list of events, at least one event having a digitally signed encrypted message associated therewith, said encrypted message comprising a descrambling key and event information including at least one of a channel identity, date and time stamp, event identity and payment amount corresponding to said associated event;
>
> receiving in said device, in response to user selection of said event, said digitally signed encrypted message;
>
> <u>authenticating a source of the digitally signed encrypted message in response to said digitally signed encrypted message</u>;
>
> decrypting said digitally signed encrypted message to obtain said descrambling key upon said authenticating;

> receiving said selected event from the service provider, said selected event being scrambled using said descrambling key for preventing unauthorized access to said selected event; and
>
> descrambling said selected event using said descrambling key. (emphasis added).

The referenced portions of Wasilewski teaches that a stream of program bearing MPEG-2 transport packets enters the SABER 20 embedded in a network protocol layer, which is then removed to access the MPEG-2 transport packets. *See, col. 11, lines 60–64.* The MPEG-2 transport packets bearing ECMs and EMMs generated by a conditional access process are then multiplexed with the transport packets that carry the content to form a single outgoing packet stream encapsulated in a network protocol destined for a user (e.g, STU 90). *See, col. 11, line 65 – col. 12, line 6.*

However, Wasilewski fails to teach any authentication step whatsoever – and clearly not "authenticating a source of the digitally signed encrypted message in response to said digitally signed encrypted message" as recited in present Claim 1. Applicant notes an analogous limitation is already present in independent Claims 15 and 18.

Further, to the extent the Office Action relies upon the updated PID discussed in col. 12, lines 17-51 of Wasilewski as being part of the recited encrypted message of Claim 1, it should be noted that this updated PID is explicitly taught to be inserted into the MPEG-2 transport packets of the program and <u>not</u> with packets having the EMM or ECM. *See, e.g., col. 12, lines 33-37.* Moreover, the packets having EMMs and ECMs are separate from the MPEG-2 transport packets used to carry audio and video data. *See, e.g., col. 11, line 65 – col. 12, line 2.*

In the Response to Arguments section of the Final Office Action, the Examiner asserts

"[t]he definition of message is a communication by signals" and concludes "[t]herefore the system of Wasilewski discloses communicating encrypted event information (column 12 lines 34-62) and descrambling key (column 12 lines 1-32)." Applicant respectfully disagrees with such an application of the term "message" to the present application. Multiple pieces of data that are separately transmitted in separate messages may not be properly considered as part of a single message. The Final Office Action provides no support whatsoever for such a broad assertion that Applicant's use of "message" in the present application equates to any arbitrary collection of communicated signals.

Applicant's use of the term "message" as recited in the present claims, should be interpreted consistently with the manner used in the specification and with its ordinary and customary meaning. It is well established that the words of a claim "are generally given their ordinary and customary meaning." *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996). The ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application." *Phillips v. AWH Corp.* (Fed. Cir. 03-1269, -1286, 9 2005) citing *Innova/Pure Water, Inc. v. Safari Water Filtration Systems, Inc.*, 381 F.3d 1111 at 1116 (Fed. Cir. 2004) ("A court construing a patent claim seeks to accord a claim the meaning it would have to a person of ordinary skill in the art at the time of the invention."). Accordingly, Applicant submits the term "message", as recited in the present claims, cannot be afforded any arbitrary meaning, but rather must be afforded the meaning it would have to a person of ordinary skill in the art as of the effective filing date of the subject patent application.

The baseline for determining the proper meaning for "message" as recited in the

present claims is the context of the particular claim in which it appears and the context of the entire patent, including the specification. *See, Phillips*, at (Fed. Cir. 03-1269, -1286, 10 2005) citing *Verve, LLC v. Crane Cams, Inc.*, 311 F.3d 1116, 1119 (Fed. Cir. 2002) and *In re Nelson*, 280 F.2d 172, 181 (CCPA 1960). In fact, the context in which a term is used in a claim can be highly instructive. *See, Phillips*, at (Fed. Cir. 03-1269, -1286, 12 2005) citing *Mars, Inc. v. H.J. Heinz Co.*, 377 F.3d 1369, 1374 (Fed. Cir. 2004) and *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1356 (Fed. Cir. 1999). To illustrate this point, the *Phillips* court pointed out that the claim at issue recited "'steel baffles,' which strongly implies that the term 'baffles' does not inherently mean objects made of steel." *Id.*. That is, a strong presumption that all baffles are not necessarily made of steel arose from the recited modification of "baffles" to require they be made of "steel".

In analogous fashion, present Claim 1 recites receiving a descrambling key and event information. Claim 1 explicitly modifies the receiving step to call for receiving "an encrypted message" that comprises both the descrambling key and event information. Accordingly, the term "message" as recited in claim 1 does not inherently mean receiving an arbitrary aggregation of the descrambling key and event information data, as argued in the present Office Action – but rather *that the descrambling key and event information are received within a common message as would be understood by one possessing ordinary skill in the pertinent art.*

Such limitation is supported by Applicant's specification, which refers to "messages" in the way that is conventionally understood by those possessing an ordinary skill in the pertinent arts. For example, Applicant submits the present specification makes clear use of the term "message", and clearly contrasts the term "message" against its conventional uses of

the terms "event" and "data" (see, e.g., specification, page 11, lines 10-18).

For example, the present specification recites, in lines 17-22, on page 10,

> EPG 580 has a unique digitally signed and encrypted message associated with each event. This message is encrypted by KSCpub and is signed using KSCpri, the private key that CA 750 assigned to EPG 580. The encrypted message may include information corresponding to the selected event and an event key KSP event.

Lines 10 – 15, on page 11 further discloses:

> After STB 100 authenticates EPG 580, the encrypted message is passed to SC 420 for decryption. SC 420 decrypts the message using KSCpri, which is stored therein, to obtain the data corresponding to the selected event and the event key. This data may include data relating to channel identity, date and time stamp, event identity, and payment amount.

Moreover, page 8, lines 24-28 reveals:

> Encrypting messages using a private key may be referred to as "signing" because anyone holding the public key can verify that the message was sent by the party having the private key. This may be thought of as being analogous to verifying a signature on a document.

Thus, in consonance with the specification, the term "message" as recited in present Claim 1 does not imply any mere aggregation of communication signals, as asserted in the Final Office Action, but rather a group of particular signals that form a message, as is conventionally understood by one possessing an ordinary skill in the art.

Accordingly, Applicant submits Wasilewski also fails to teach at least the recited "encrypted message comprising a descrambling key and event information", in addition to the recited authentication step, of Claim 1.

The combined referenced teachings of Wasilewski and Hendricks fail to remedy these

shortcomings of Wasilewski. First, Hendricks was not relied upon in rejecting previous Claim 15 – which explicitly recited an authentication analogous to that of amended Claim 1. Further, Applicant notes Hendricks is not relied upon in the Final Office Action as teaching the recited encrypted message. The Final Office Action instead attempts to rely upon Wasilewski in this regard. Accordingly, as recognized by the Final Office Action, the referenced teachings of Hendricks fail to remedy at least the aforementioned shortcomings of Wasilewski.

Further, the combined referenced teachings of Wasilewski and Pinder (U.S. Pat. No. 5, 742,677) also fail to remedy the aforementioned shortcomings of Wasilewski. First, with regard to the recited authentication, in rejecting previous Claim 15, the Final Office Action attempts to remedy the shortcoming of Wasilewski by arguing, "Pinder discloses the use of the private key used for digital signatures" in column 5, lines 33-34. *See, 5/19/2005 Final Office action, pg. 5, lines 12-20.* A detailed reading of Pinder reveals that, while Pinder may generally disclose signing service authorizations, the sentence that includes lines 33-34 of column 5 of Pinder states,

> "[t]hese commands then are received, decrypted using also the subscribers private key and authorization data is stored in the secure terminal memory."

Thus, the referenced portion of Pinder explicitly teaches decrypting an authorization data using a private key. However, this does not serve to provide for any authentication, but instead teaches restricting access to intended recipients. That is, a private key cannot be used to authenticate a source of any encrypted message, as its very use requires the message was encrypted using the corresponding public key. As public keys are by their very nature publicly available, such a process merely restricts access to the encrypted data to those

possessing the corresponding private key and cannot be used to authenticate the source of the encrypted message. Rather, in order to allow one to authenticate a source of an encrypted message, the message must be encrypted using a private key, such that anyone having access to the corresponding public key can confirm the message was encrypted using the private key, (e.g., is authentic).

Accordingly, the combined teachings of Wasilewski and Pinder also fail to teach at least the recited authentication step of Claim 1. Further, Applicant notes the Final Office Action relied only upon Wasilewski to allegedly teach the "encrypted message" recitation of Claim 1. Pinder fails to add anything to Wasilewski in this regard. For purposes of completeness, Applicant also submits Vancelette (U.S. Pat. No. 5,894,320) fails to cure the above-identified deficiencies of the proposed combination of references.

In view of the foregoing, Applicant respectfully requests reconsideration and removal of the rejection of Claim 1, as the cited art of record fails to teach each of the recited limitations thereof – namely, at least the recited authentication and encrypted message of Claim 1. Applicant further requests reconsideration and removal of the rejections of Claims 2-14 at least by virtue of these claims' ultimate dependency upon a patentably distinct base Claim 1.

Rejection of Claim 15 under 35 USC 103(a) as being unpatentable over Wasilewski (U.S. Patent 6,424,714) in view of Pinder (U.S. Patent 5,742,677)

Applicant further requests reconsideration and removal of the rejection of Claim 15 as being unpatentable over Wasilewski in view of Pinder. First, with regard to Claim 15, the

Final Office Action asserts in the Response to Arguments section that:

> Applicant argued that claim 15 recites a symmetric key encrypted using public key cryptography. However, claim 15 recites "... decrypting, in said smart card, said message using a private key ... to obtain a symmetric key ..." Claim 15 discloses the public key is used for decrypting said digital signature. The use of a public key is used in an asymmetric key encryption process as opposed to a symmetric key encryption.

In response, Applicant notes Claim 15 calls for: (1) authenticating a guide provider using a public key to decrypt a signature; (2) using a private key to decrypt a message containing a symmetric key; and, (3) descrambling an event using the decrypted symmetric key. Thus, Claim 15 indeed calls for a symmetric (descrambling) key encrypted using public key (asymmetric) cryptography.

More particularly, Claim 15 (in similar fashion to Claim 1) recites:

> A method for managing access between a device having a smart card coupled thereto and a service provider, said device performing the steps of:
>
> receiving an electronic program guide from a guide provider, *said guide having a message and a digital signature associated with each event in said guide, said message being encrypted using a public key of the smart card and said digital signature being created using a private key of said guide provider*;
>
> selecting an event from said guide;
>
> receiving said encrypted message and said digital signature corresponding to the selected event;
>
> *authenticating said guide provider by decrypting said digital signature using a public key of said guide provider, said guide public key being stored in said device*;
>
> passing said message to said smart card;
>
> *decrypting, in said smart card, said message using a private key of said smart card to obtain event information and a symmetric key*, said smart card private key being stored within said smart card;
>
> storing said event information in said smart card and updating account information based on said event information;

> receiving from the service provider said selected event, said selected event being scrambled using said symmetric key; and
>
> descrambling, in said smart card, said selected event using said symmetric key to generate a descrambled event. (*Emphasis added*).

Thus, Claim 15 recites in part the steps of decrypting an encrypted message to obtain event information and a symmetric key, which symmetric key is then used to descramble an event. While the Wasilewski reference may teach encrypting control words using a multi-session key (MSK), the reference does not teach either the recited authentication nor an encrypted message that comprises a descrambling key and event information. Thus, the arguments discussed hereinabove with regard to Claim 1 also apply to present independent Claim 15. The Pinder reference fails to overcome the deficiencies associated with Wasilewski as discussed above.

In view of the foregoing, Applicant respectfully requests reconsideration and removal of this 35 USC 103 rejection of Claim 15. Applicant also requests reconsideration and removal of the rejections of Claims 16 and 17, at least by virtue of these claims' ultimate dependence from patentably distinct base Claim 15.

Rejection of Claim 18 under 35 USC 103(a) as being unpatentable over Wasilewski (U.S. Patent 6,424,714) in view of Pinder (U.S. Patent 5,742,677)

Applicant further requests reconsideration and removal of the rejection of Claim 18 as being unpatentable over Wasilewski in view of Pinder. Claim 18 recites:

> A method for managing access between a device having a smart card coupled thereto and a service provider, said device performing the steps of:
>
> receiving an electronic program guide from a guide provider, said guide having a digital certificate and a separate message corresponding to each event in said guide, each of said

> digital certificates being encrypted using a first private key of said guide, said separate message being encrypted using a public key of the smart card and having an associated digital signature created using a second private key of said guide;
>
> selecting an event from said guide;
>
> *receiving said digital certificate, said message and said digital signature corresponding to the selected event*;
>
> *authenticating said guide provider by decrypting said digital certificate using a first public key of said guide to obtain a second public key of said guide, and decrypting said digital signature using said second guide public key, said first guide public key being stored in the device*;
>
> passing said message to said smart card;
>
> *decrypting, in said smart card, said message using a private key of the smart card to obtain event information and a symmetric key, said smart card private key being stored within the smart card*;
>
> storing said event information in the smart card and updating account information based on said event information;
>
> receiving from the service provider said selected event, said selected event being scrambled using said symmetric key; and
>
> descrambling, in said smart card, said selected event using said symmetric key to generate a descrambled event. (*Emphasis added*).

As discussed above with regard to independent Claims 1 and 15, none of the cited references of record, either alone or in combination, teach or suggest each of the recited features and limitations of present Claim 18. Reconsideration and removal of the rejection of Claim 18 is requested for at least the reasons set forth with regard to Claims 1 and 15. Applicant also requests reconsideration and removal of the rejections of dependent Claims 19 and 20, at least by virtue of these Claims' ultimate dependence from patentably distinct base Claim 18.

Conclusion

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, Claims 1-20 of this application stand in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicant's attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully Submitted
AHMET M. ESKICIOGLU

Date: August 31, 2005

Paul Kiel, Attorney
Registration No. 40,677

THOMSON LICENSING INC.
Patent Operations
CN 5312
Princeton, NJ 08543-0028

CERTIFICATE OF MAILING

I hereby certify that this amendment is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia, 22313-1450 on

August 31, 2005
Date

Linda Tindall